RANSOMWARE GUÍA DE APROXIMACIÓN

QUÉ ES EL RANSOMWARE

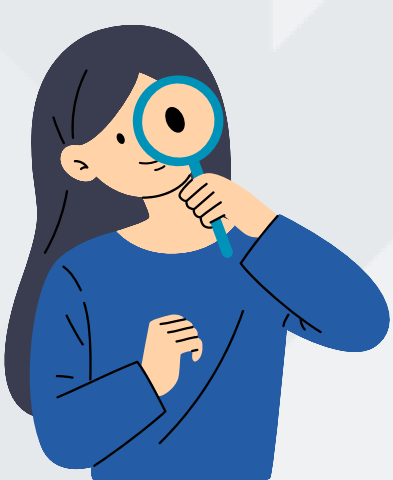
Software que **impide el acceso** a nuestra información o **amenaza** con **destruirla o divulgarla** en caso de **no acceder al pago** de un **rescate**.

CÓMO PUEDO PROTEGERME

- **Revisa** con atención **los correos** que recibas. No actúes de manera impulsiva y, ante cualquier sospecha, **informa al CAU** y/o **Dpto. de Seguridad**.
- **Desconfía** de **correos** recibidos de **desconocidos** o que contengan **vocabulario o expresiones poco corrientes** o **faltas de ortografía**. Desconfía también de aquellos que aparentan ser **urgentes** y que requieren nuestra acción inmediata. En **ningún caso respondas a dichos correos** o **abras sus adjuntos.**
- Ten **precaución al descargar o abrir ficheros adjuntos a correos** con asuntos tipo “factura”, “multa”, “recibo”, “paquete no entregado” aunque provengan de contactos conocidos, podrían haber suplantado a alguno de tus contactos.
- Ten **precaución al pulsar en enlaces** facilitados en un correo aunque, en apariencia, sean de contactos conocidos o terceras partes de confianza, especialmente si corresponden a **direcciones desconocidas o sospechosas**.
- **Evita ejecutar las macroinstrucciones** (”macros”) de los archivos recibidos, **a no ser que estés completamente seguro de su procedencia**.

CÓMO ACTUAR EN CASO DE SER ATACADO

- **No pagues** nunca el **rescate**.
- **Desactiva el Wi-Fi** o **desconecta el cable de red del dispositivo** atacado.
- **Avisa** inmediatamente al **CAU** y/o **Dpto de Seguridad** de tu organismo.



Junta de Andalucía